

Time Stamp ръководство на потребителя **Версия 1.6**

Информационно обслужване АД разполага с налични ресурси за издаване на електронни удостоверения за време чрез своя **Time Stamp Server**. За момента в България това е една почти непозната услуга, за която няма подходящи клиентски реализации, позволяващи на бизнеса, гражданите и държавните институции да се възползват ефективно от нея.

TimeStamp има за цел да запълни тази нужда.

Системата дава възможност на регистрираните потребители да получават удостоверения за време за избран от тях документ, който се намира на локалния им компютър. Впоследствие ще се поддържа онлайн регистър на издадените удостоверения, в който ще може да се търси и доказва подписване по време от всеки Интернет потребител. Възможно е да се реализира и подписване по време на онлайн съдържание (уеб страници и др.) през определен интервал, доказващо времето на изнасяне на информация.

Системата е уеб базирана, разделена на модули, всеки от които ще бъде със специфично предназначение и функционалност. Ще се използва оторизация на базата на електронни сертификати, като ще се допуска използването единствено на удостоверения за ЕП на Информационно Обслужване АД.

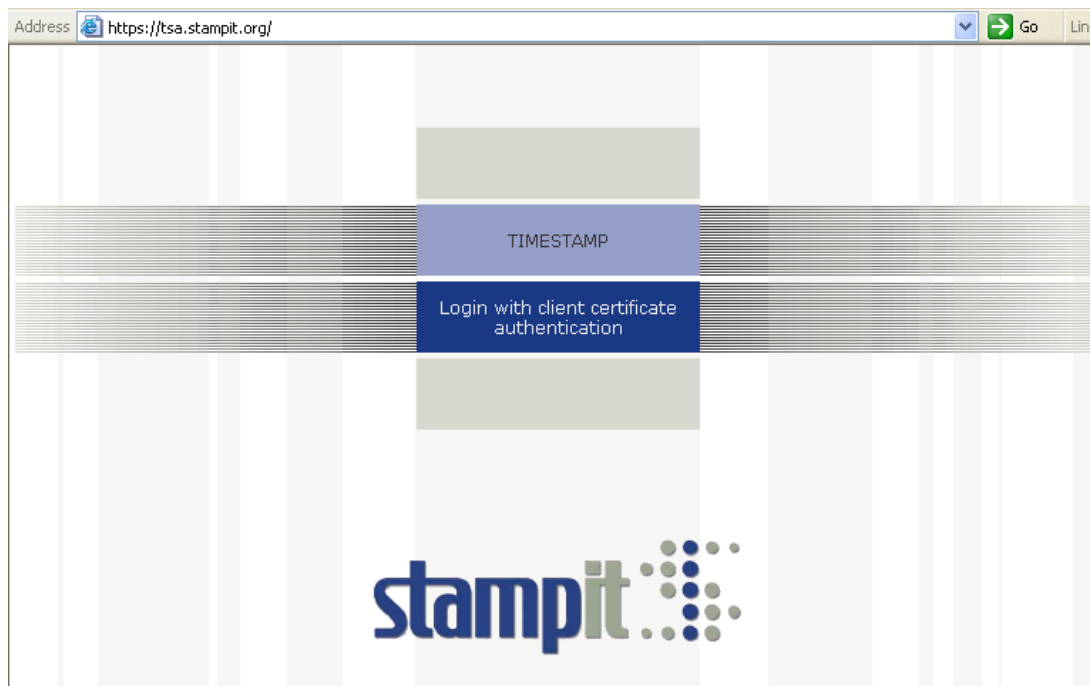
Работа с online приложението за удостоверяване на време.

Основните функции, достъпни за клиенти са:

- Удостоверяване на време
- Удостоверяване на време (опростен вариант)
- Търсене
- Състояние на сметката
- Изход.

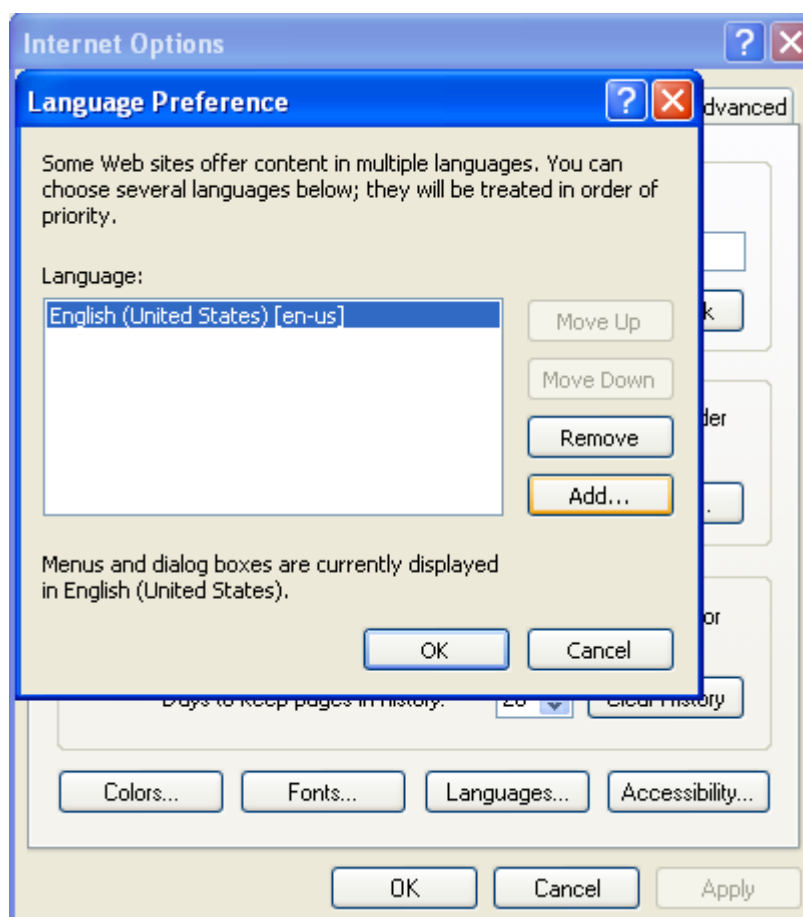
1. Вход в системата.

При първоначално зареждане на приложението ще видите следния екран:



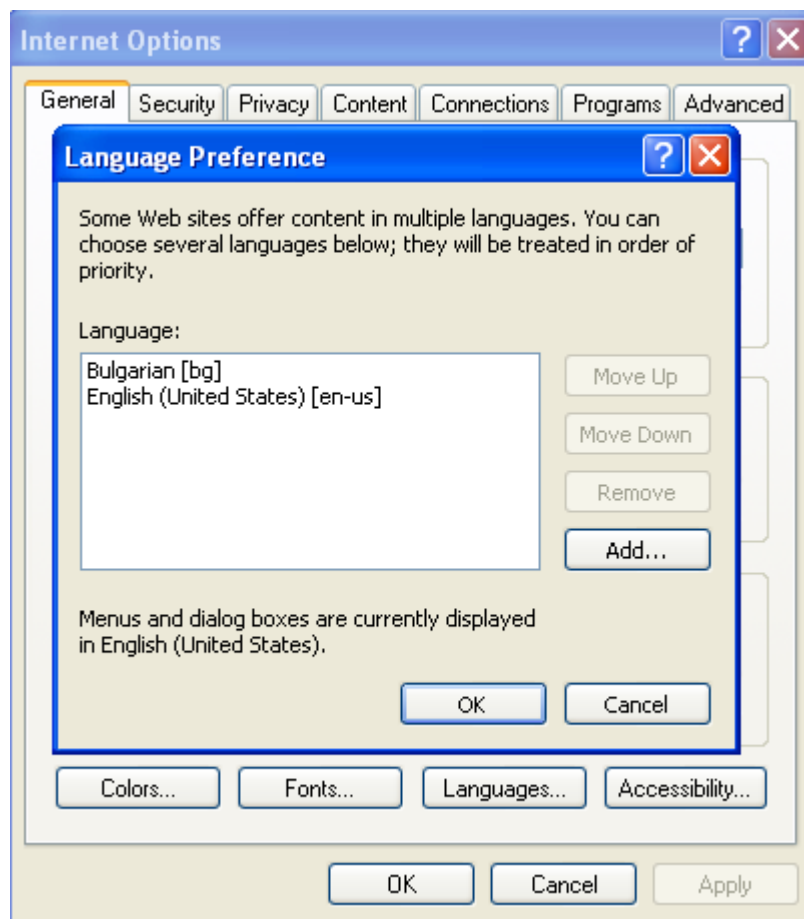
фиг. 1

Ако желаете текста в менютата да Ви е на кирилица натиснете последователно **<Tools>**, **<Internet Options...>** и натиснете бутона **<Languages>**. Ще видите следния прозорец:



фиг. 2

Ако липсва **<Bulgarian[bg]>** натиснете бутона **<Add...>** и го добавете, след което с маркиране и бутона **<Move Up>** трябва да е най-отгоре. /фиг. 3/.



фиг. 3

Потвърдете с <ОК>, затворете всички отворени браузери и отворете отново. След успешна настройка трябва да видите следния екран./фиг. 4/



фиг. 4

- Натиснете <Вход с представяне на клиентски сертификат>



фиг. 5

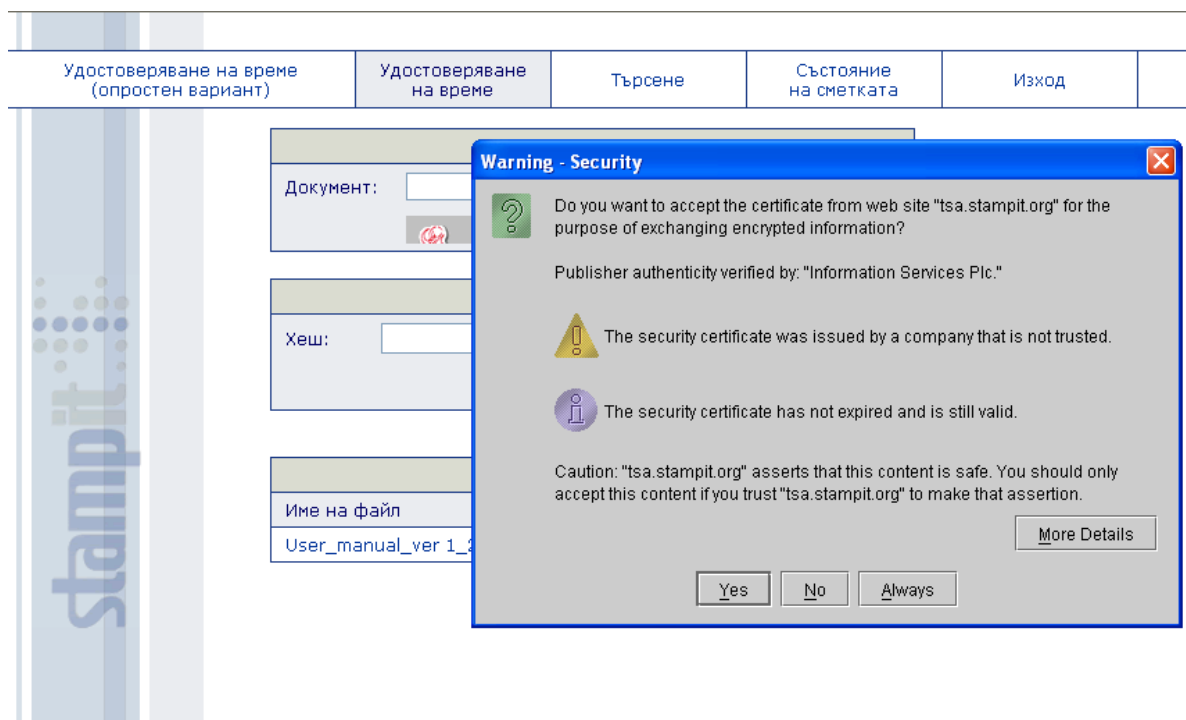
- изберете с кой сертификат ще се оторизирате /фиг.5/



фиг. 6

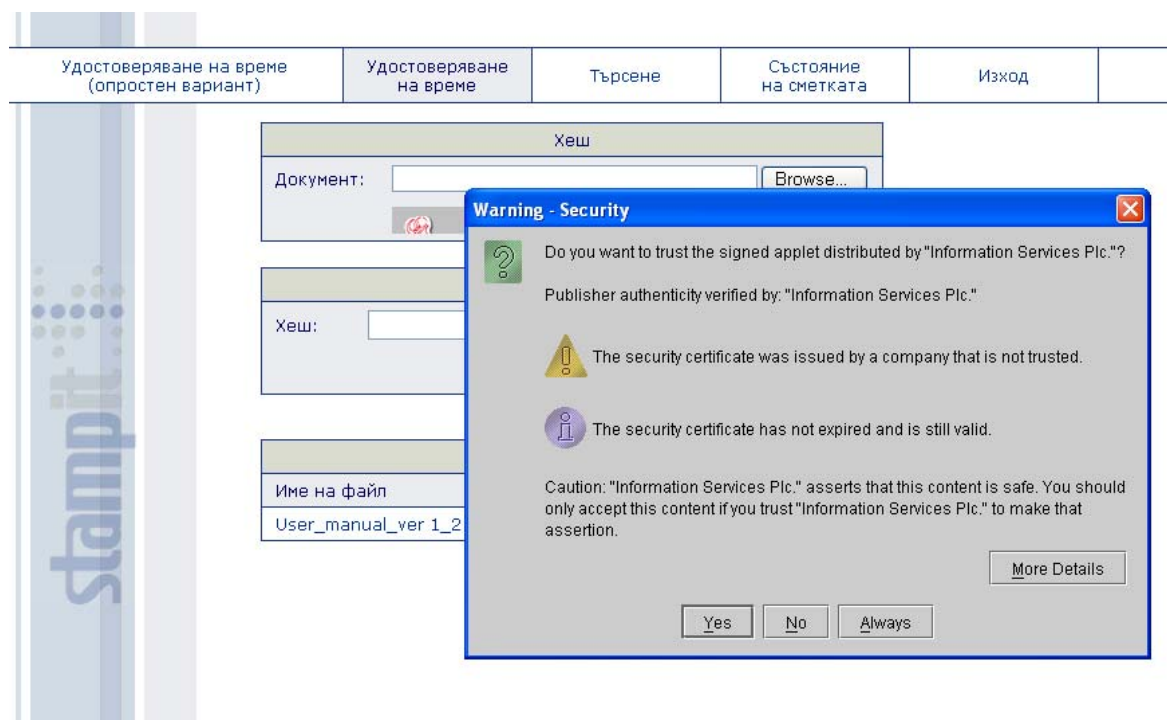
- въведете пин кода на вашата смарт карта

Ще видите прозорец подобен на този на <фиг. 7>



фиг. 7

Натиснете **'Always'** ако искате този прозорец да не се показва всеки път при влизане в системата.



фиг. 8

Удостоверяване на време (опростен вариант)	Удостоверяване на време	Търсене	Състояние на сметката	Изход
---	----------------------------	---------	--------------------------	-------

Хеш

Документ:

Заявка

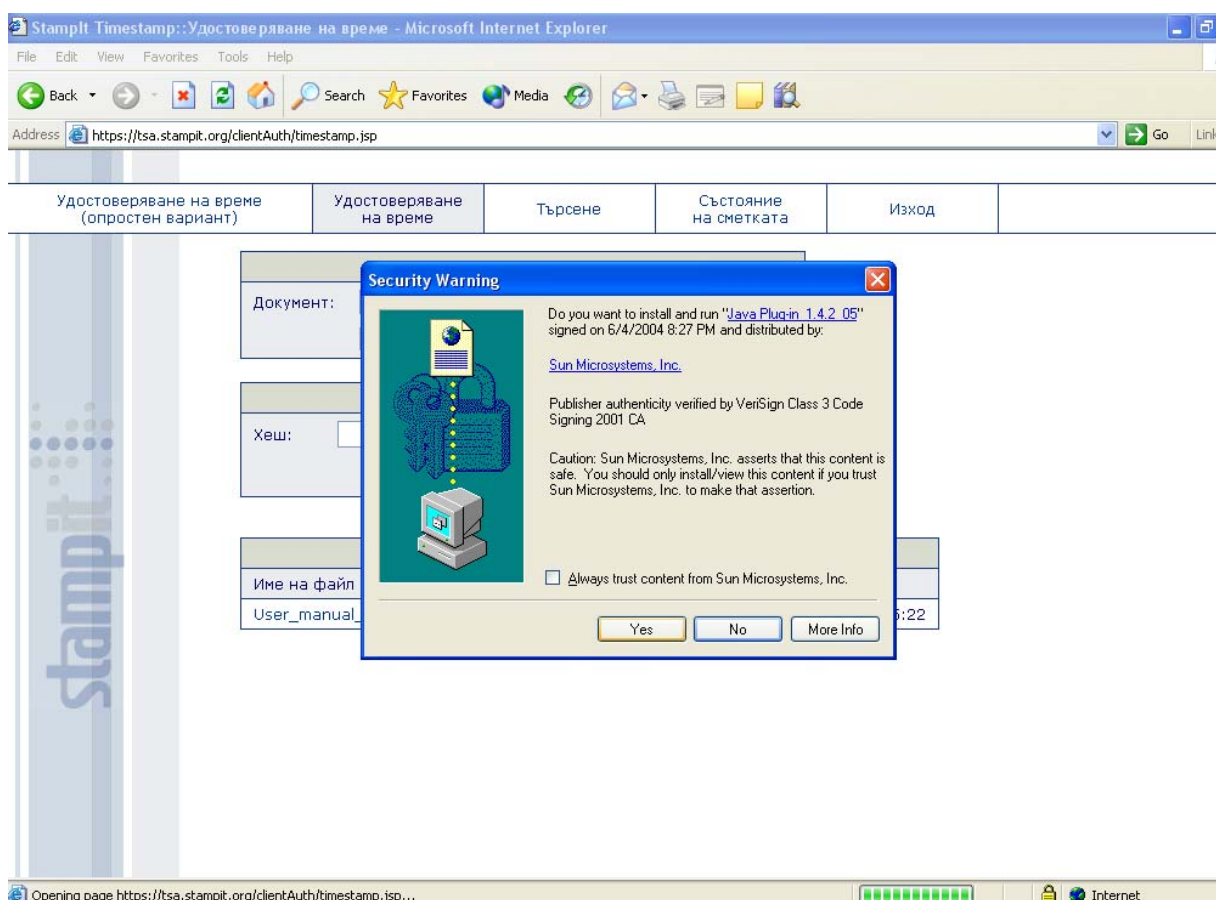
Хеш:

Последни заявки

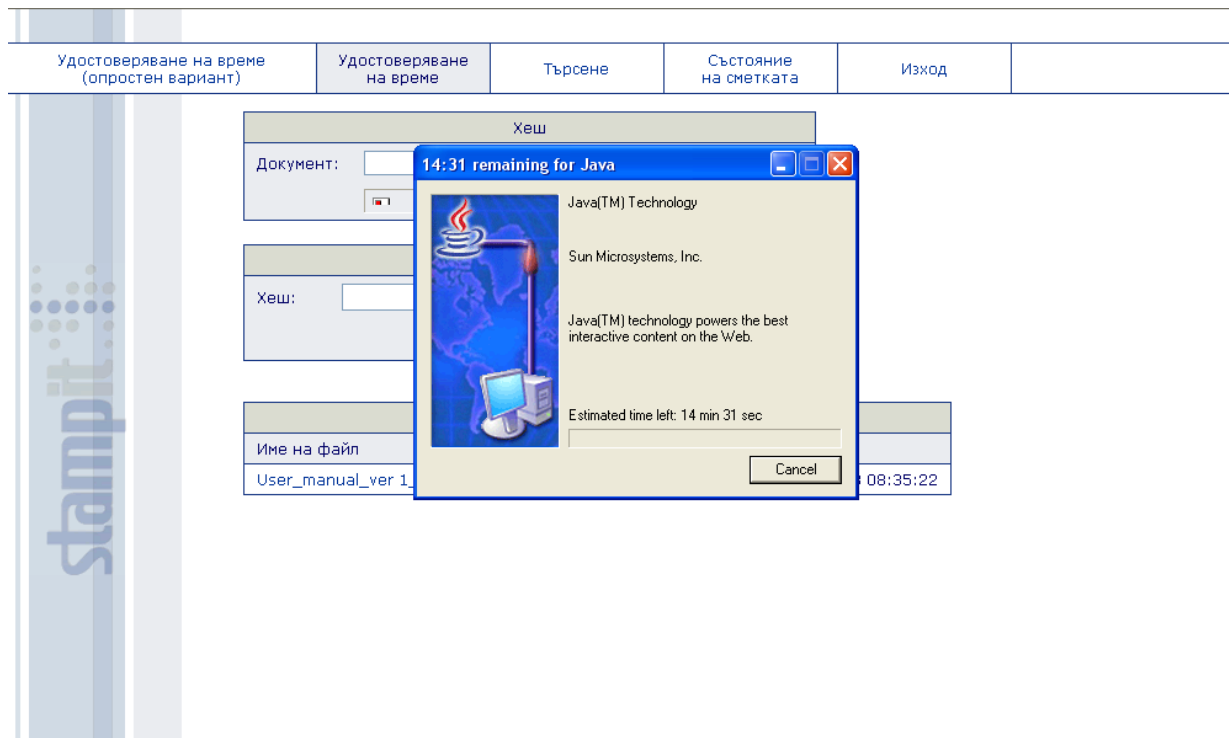
Име на файл	Хеш	Зулу време
User_manual_ver 1_2.pdf	rusJhVh2E6Iu3mTJDPgFeCKLVEA=	2004/08/23 08:35:22

фиг. 9

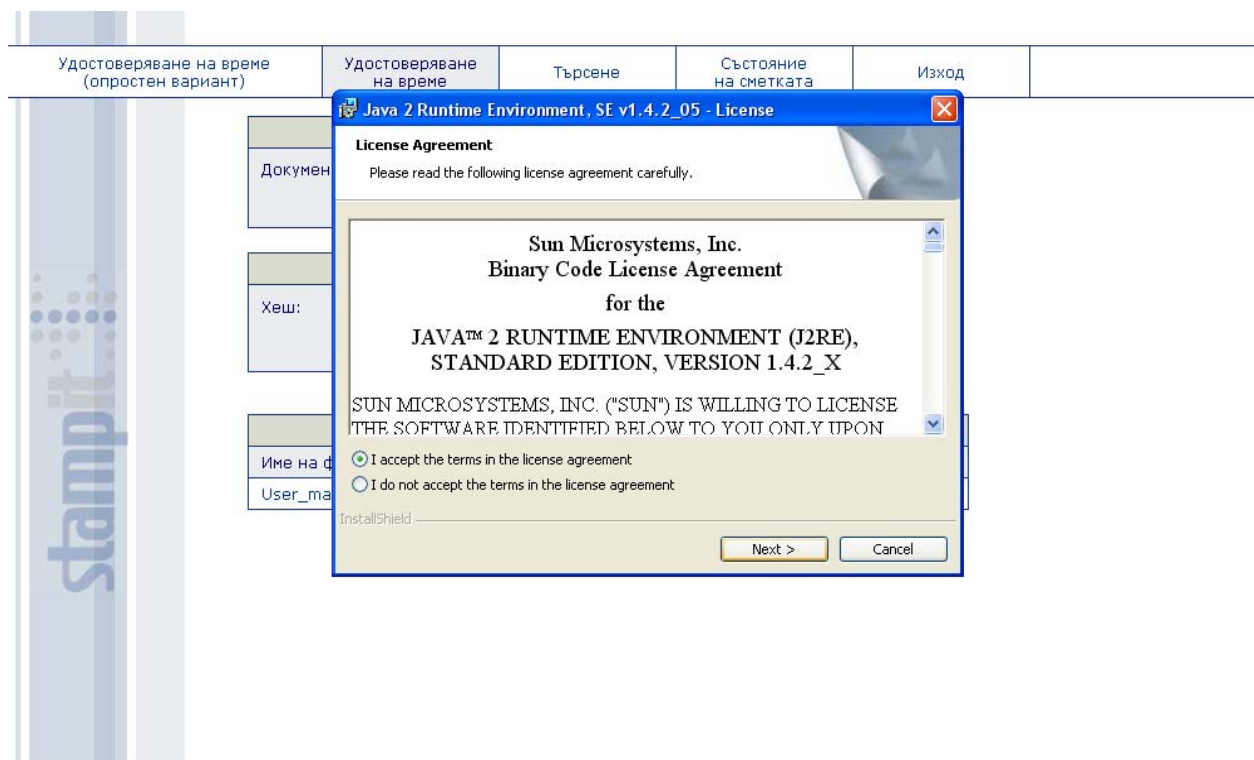
Ако нямате инсталиран **"Java Plug-in"** приложението ще Ви предложи инсталация /фиг.10/. Потвърждавате с **<Yes>** и ще преминете през следните прозорци. /фиг.11, фиг.12, фиг.13 и фиг.14/



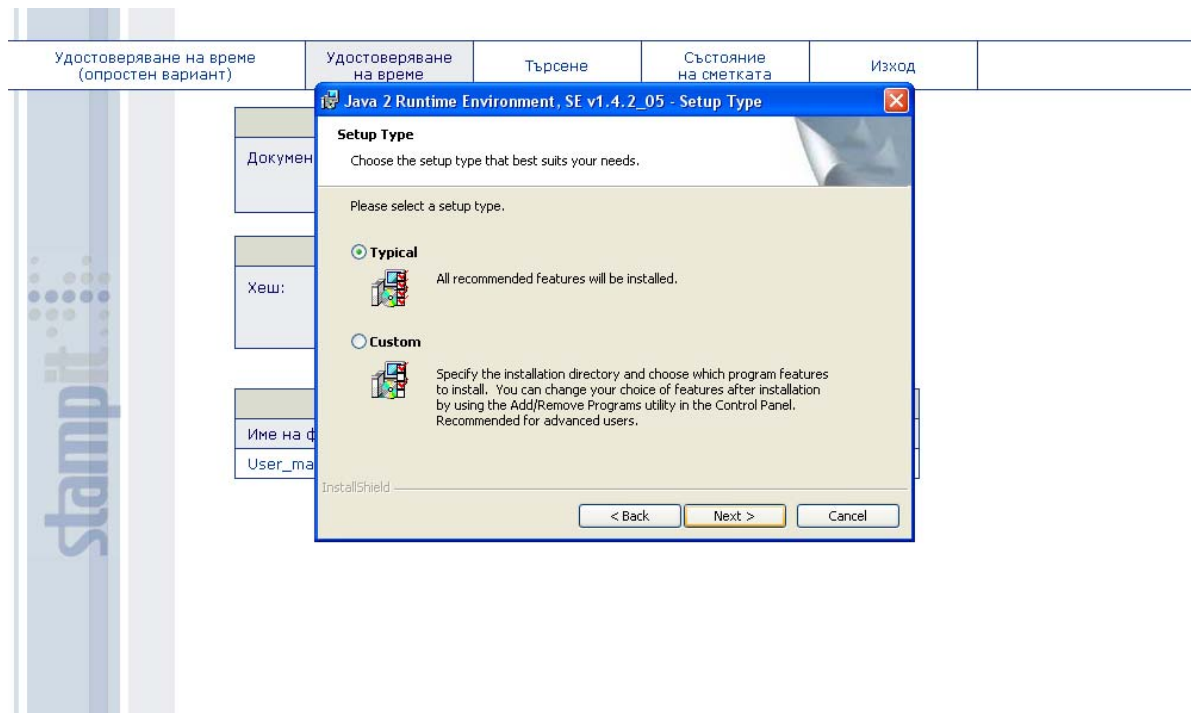
фиг. 10



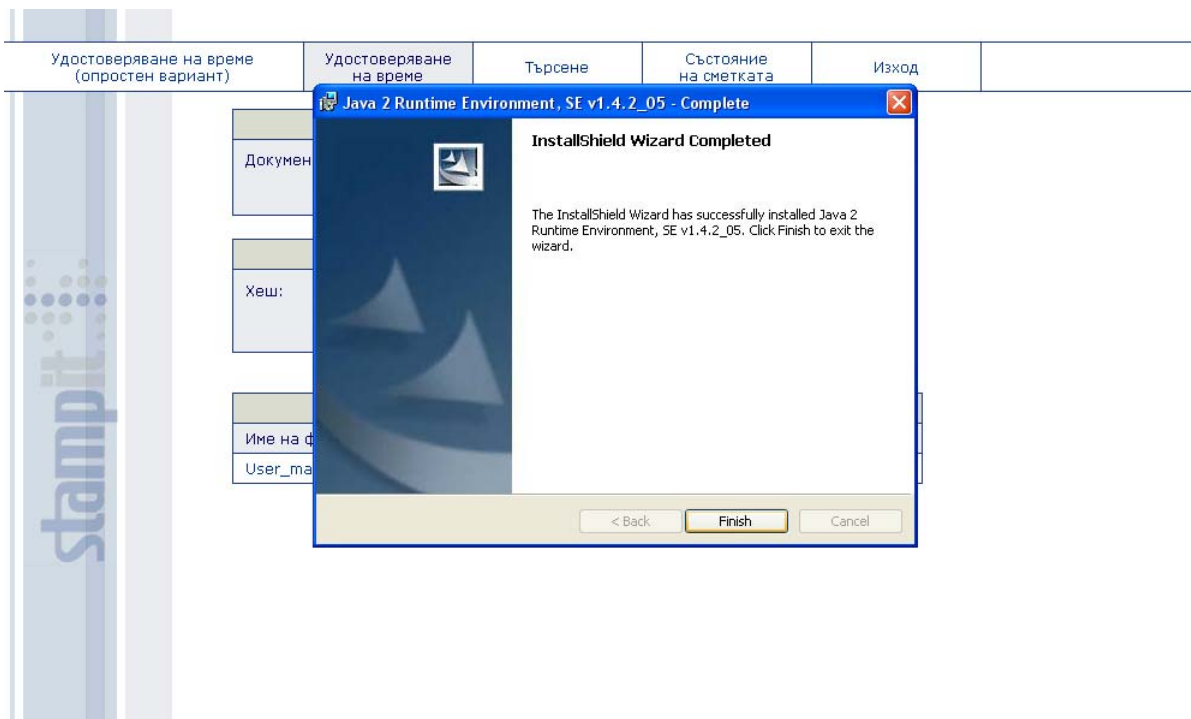
фиг. 11



фиг. 12



фиг. 13



фиг. 14

2. Удостоверяване на време.

По подразбиране след вход в системата е установена функцията Удостоверяване на време /фиг.15/. За да се удостовери по време определен документ, намиращ се на клиентския компютър, е необходимо следното:

- Посочете пълния път до документа или с бутона <**Browse...**> го селектирайте /фиг. 15/.
- Натиснете бутона <**Пресмятане на хеш**>, който изчислява SHA1 (base64 кодиран) хеш на документа.
- Натиснете бутона <**TimeStamp**>. Бутонът <**TimeStamp**> генерира Time Stamp Query базиран на пресметнатия хеш и го праща до Time Stamp Server-а на доставчика. Сървърът подписва заявката и връща подписан Time Stamp

Response. Клиентът може да запише отговора на сървъра под формата на файл (с разширение .tsr). Удостоверената по време заявка се записва в база данни. /фиг. 15/.

Важно за клиента е да знае, че документа, за който се удостоверява време, не се изпраща към удостоверяващия орган, а само хеш от този документ.

Удостоверяване на време (опростен вариант)	Удостоверяване на време	Търсене	Състояние на сметката	Изход									
Хеш Документ: C:\rute.pdf Browse... Пресмятане на хеш Заявка Хеш: JtmYUi7mfjv2Y9DDH13AEHudbw= Timestamp Последни заявки <table border="1"> <thead> <tr> <th>Име на файл</th> <th>Хеш</th> <th>Зулу време</th> </tr> </thead> <tbody> <tr> <td>rute.pdf</td> <td>JtmYUi7mfjv2Y9DDH13AEHudbw=</td> <td>2004/09/02 06:37:13</td> </tr> <tr> <td>rute.pdf</td> <td>JtmYUi7mfjv2Y9DDH13AEHudbw=</td> <td>2004/09/02 06:31:07</td> </tr> </tbody> </table>					Име на файл	Хеш	Зулу време	rute.pdf	JtmYUi7mfjv2Y9DDH13AEHudbw=	2004/09/02 06:37:13	rute.pdf	JtmYUi7mfjv2Y9DDH13AEHudbw=	2004/09/02 06:31:07
Име на файл	Хеш	Зулу време											
rute.pdf	JtmYUi7mfjv2Y9DDH13AEHudbw=	2004/09/02 06:37:13											
rute.pdf	JtmYUi7mfjv2Y9DDH13AEHudbw=	2004/09/02 06:31:07											

фиг. 15

3. Търсене

Функцията търсене дава възможност на потребителя да търси в базата данни дали определен документ е бил удостоверен по време. Търсенето се извършва по хеш на документа. Вариантите в случая са два:

- ако разполагаме с документа, можем да посочим пълния път до него/или с бутона **<Browse...>** го селектираме/, след това се натиска бутона **<Пресмятане на хеш>**.
- ако знаем хеша, да го изпишем в полето **<Хеш:>**.

Избират се допълнителни опции за търсене по време и се натиска бутона **<Търсене>**. Може да се избере дата, като критериите за търсене са дали има удостоверен по време документ преди тази дата, след тази дата или между две дати. Опцията **<без значение>** ще покаже всички открити документи със съответстващ хеш, без значение от времето на удостоверяване. /фиг. 17/

Удостоверяване на време (опростен вариант)	Удостоверяване на време	Търсене	Състояние на сметката	Изход	
---	----------------------------	---------	--------------------------	-------	--

Хеш

Документ: C:\rute.pdf

Документ

Хеш: JtmYUi7mfjyv2Y9DDH13AEHudbw=

Име на файл:

Дата (дд/мм/гггг)

☒ без значение
☐ преди
☐ след
☐ между и

фиг. 16

Удостоверяване на време (опростен вариант)	Удостоверяване на време	Търсене	Състояние на сметката	Изход	
---	----------------------------	---------	--------------------------	-------	--

Ново търсене

Резултати от търсенето

2 заявки отговарят на търсенето

Резултати 1 - 2

Име на файл	Хеш	Зулу време	Потребител
rute.pdf	JtmYUi7mfjyv2Y9DDH13AEHudbw=	2004/09/02 06:37:13	Stefan Todorov Karastoyanov
rute.pdf	JtmYUi7mfjyv2Y9DDH13AEHudbw=	2004/09/02 06:31:07	Stefan Todorov Karastoyanov

Хеш

Документ:

Документ

Хеш: JtmYUi7mfjyv2Y9DDH13AEHudbw=

Име на файл:

Дата (дд/мм/гггг)

☒ без значение
☐ преди

фиг. 17

За да разгледате детайли за удостоверяването по време, изберете резултата от търсенето, който Ви интересува. Имате възможност да запишете под формата на файл заявката и отговора за Time Stamp Server, както и да разпечатате отговора на принтер.
/фиг. 18/

stampit

Удостоверяване на време (опростен вариант)	Удостоверяване на време	Търсене	Състояние на сметката	Изход	
Данни на заявката					
Пореден номер	17				
Потребител	Stefan Todorov Karastoyanov				
Име на файл	rute.pdf				
Хеш	JtmYUi7mfjyv2Y9DDH13AEHudbw=				
Дата/време	2004/09/02 06:37:13				
Детайли на заявката		Съхранение на заявката			
Policy					
Nonce					
Искане на сертификата на TSA	true				
Хеш алгоритъм	1.3.14.3.2.26				
Верификация на Timestamp token	Подписът е ок Съхранение на TSA сертификата				
Детайлни на отговора		Съхранение на отговора 			
Статус	0				
Статусни редове	Time stamped successfully				
Policy	1.3.6.1.4.1.11290.1.1.2				
Сериен номер	35				
Зулу време	2004/09/02 06:37:13.967				
Ordering	false				
Nonce					

фиг. 18

За да разгледате детайлите на клиентския сертификат, с който е подадена заявката за удостоверяване на време, изберете името на потребителя. /фиг. 19/, след което ще се отвори прозорец подобен на този от **фиг. 20**.

Удостоверяване на време (опростен вариант)	Удостоверяване на време	Търсене	Състояние на сметката	Изход	
---	----------------------------	---------	--------------------------	-------	--

stampit

Ново търсене

Резултати от търсенето

1 заявка отговаря на търсенето Резултати 1 - 1

Име на файл	Хеш	Зулу време	Потребител
User_manual_ver 1_2.pdf	rusJhVh2E6Iu3mTJDPgFeCKLVEA=	2004/08/23 08:35:22	Elin Todorov Koley

Хеш

Документ:

Документ

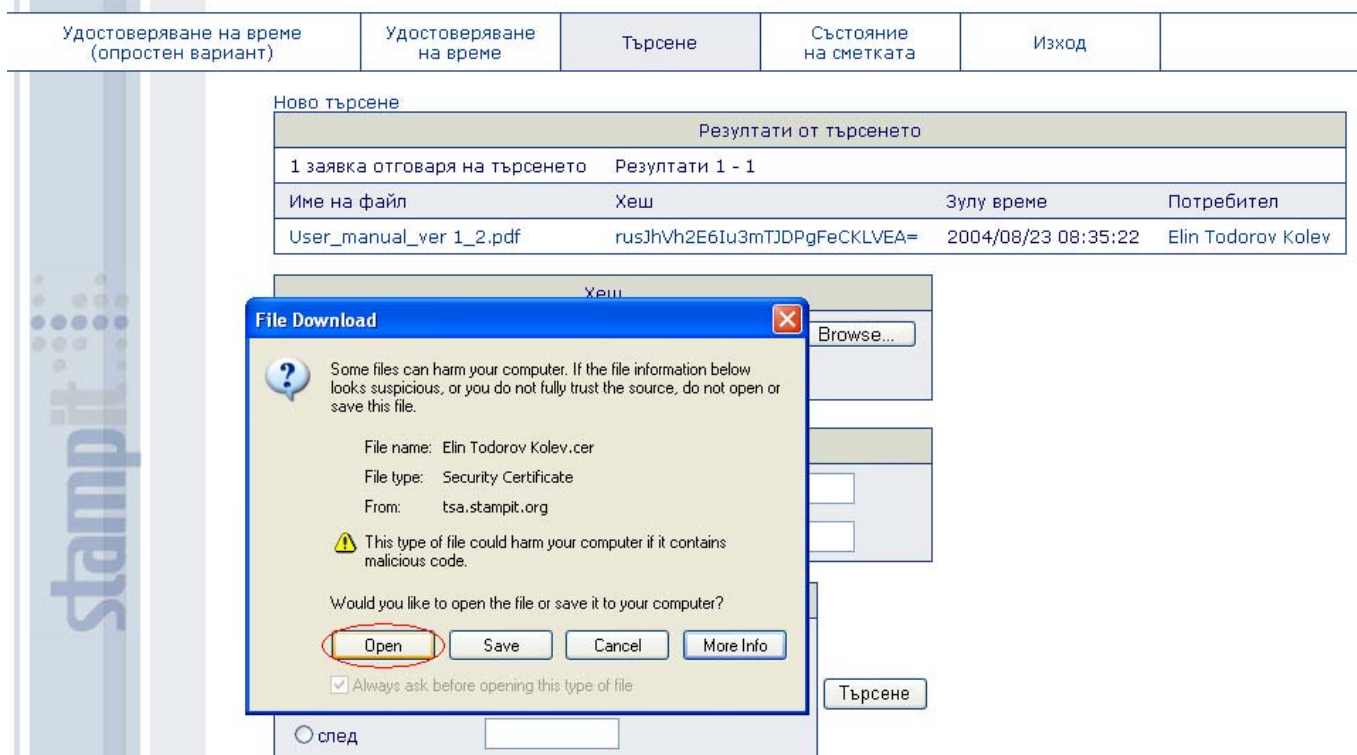
Хеш:

Име на файл:

Дата (дд/мм/гггг)

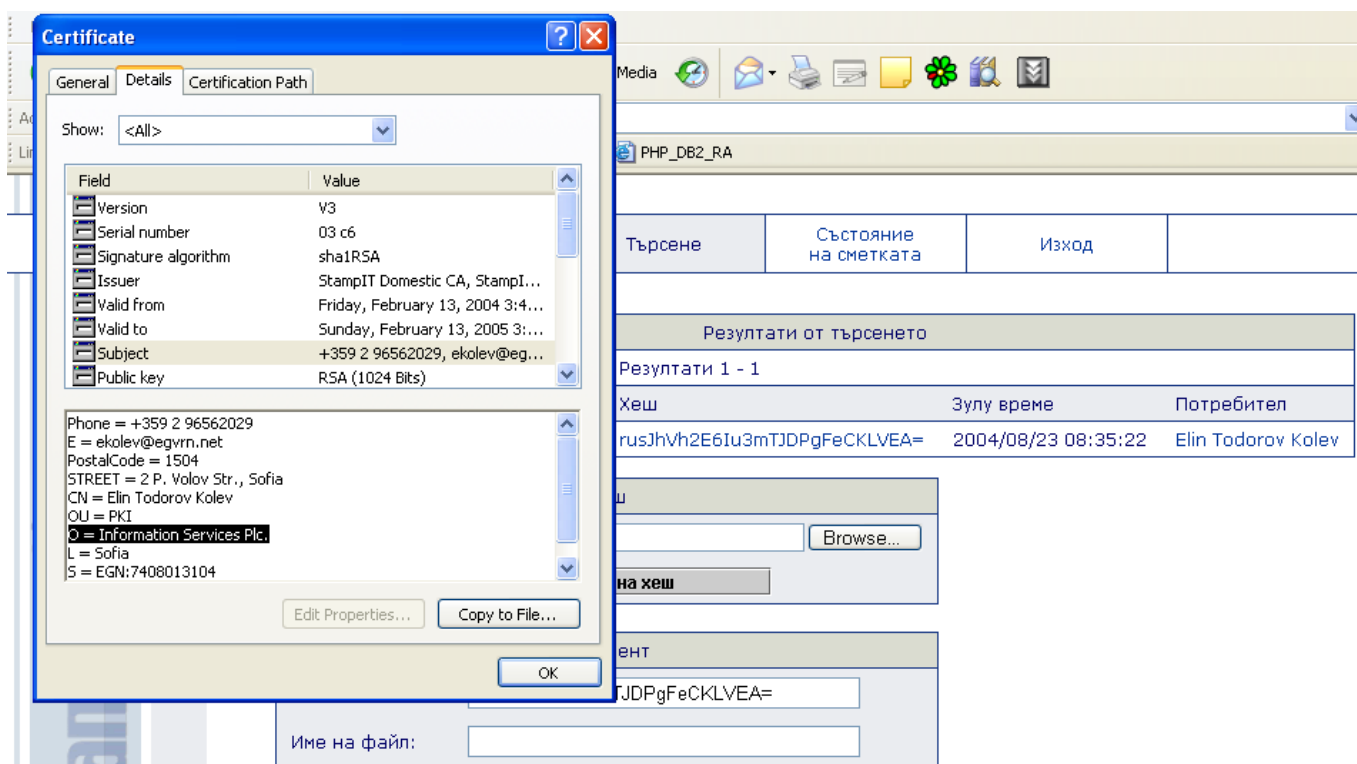
☒ без значение
☐ преди
☐ след

фиг. 19



фиг. 20

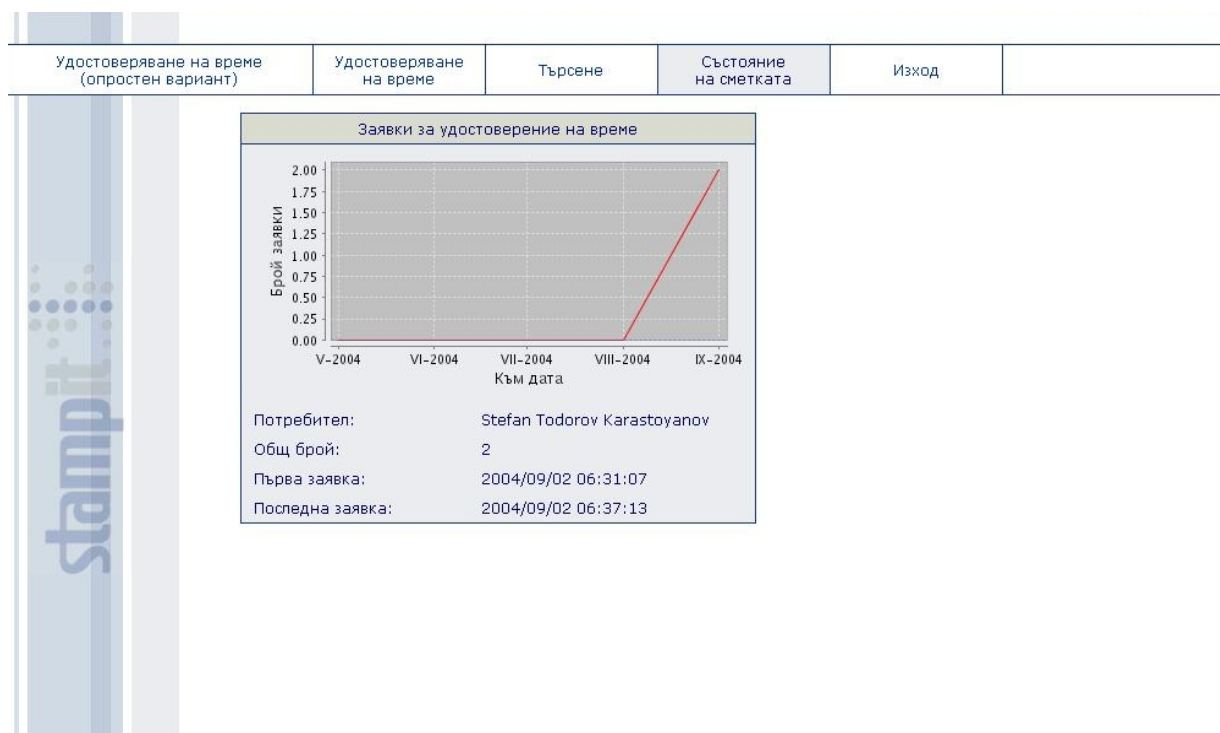
Избира се **<Отвори>**, след което можете да разгледате детайлите на сертификата./фиг. 21/



фиг. 21

4. Състояние на сметката

Състояние на сметката Ви дава информация за направените от Вас заявки за удостоверяване на време, дата на първата заявка, дата на последната заявка, брой заявки и графика, показващата честотата на направените заявки. /фиг. 22/



фиг. 22

5. Удостоверяване на време (опростен вариант)

Функцията Удостоверяване на време (опростен вариант) – ви дава възможност да удостоверите време чрез предварително изчислен хеш на документ или предварително подготвен .tsq файл.

Удостоверяване на време (опростен вариант)	Удостоверяване на време	Търсене	Състояние на сметката	Изход	
Заявка SHA1 хеш на документ (base64 кодиран): RFC #3161 .tsq файл: Browse... Timestamp					

фиг. 20